AWARENESS BRIEF

Computer Security

The challenge of keeping information systems secure

Editor's Note:

A previous CSIS Liaison / Awareness Brief *Economic Espionage: The Risk of Conducting Business in the International Marketplace* (April 1998), identified some economic espionage methodologies used to disadvantage Canadian interests. The purpose of this brief is to highlight some of the computer security issues that impact upon individuals and organizations who rely more and more on information technology to conduct business. The vulnerability of Canadian organizations to acts of economic espionage can be reduced through timely information about computer security issues and the adoption of computer security practices.

This brief is published as part of CSIS's national Liaison/Awareness Program. Through this program, the Service seeks to establish ongoing dialogue with organizations, both public and private, concerning the threat posed to Canadian interests by foreign government involvement in economic espionage.

Introduction

Advances in telecommunications and in computer technology have caused an information revolution, the impact of which may be as profound as that of the industrial revolution of the nineteenth century. The rapid evolution of telephone, cable, satellite and computer networks and software, combined with technological breakthroughs in computer processing have made this latest revolution possible.

Apart from the rapid evolution of personal computers (PCs), the computing environment today allows for a sophisticated and complex interconnection of PCs, networks and hosts. Many organizations now have PCs connected to different networks with the additional capability of accessing a mainframe. Laptops and notebook computers add to the risk factor by providing the ability to easily remove sensitive information from the workplace. The loss of sensitive information, whether deliberate or inadvertent, can carry a price tag far beyond the cost of platform hardware.

The Internet

The Internet is a global network interconnecting thousands of dissimilar computer networks and millions of computers worldwide. Over the past 20 years, it has evolved from its relatively obscure use by scientists and researchers to its significant role today as a popular, user-friendly and cost-effective means of communication and information

exchange. Millions of people conduct business over the Internet, and millions more use it for entertainment.

Internet use has been more than doubled annually for the last several years to an estimated 40 million users in nearly every country today. Connections are growing at an ever increasing rate with the Internet adding a new network about every 30 minutes.

Because the Internet strives to be a seamless web of networks, it is virtually impossible today to distinguish where one network ends and another begins. Local, provincial and federal government networks, for example, are interconnected with commercial networks, which in turn are interconnected with military networks, financial networks, utilities networks and so on.

The only equipment required for Internet access is a PC with a modem and a telephone line. As more people get connected, the attractiveness of the Internet as a convenient, cheap, quick and intriguing way of communicating increases. With more participants, the amount of available information (news groups, program and data files, graphic and multimedia documents, and government and industry documents) increases and attracts even more users.

Security problems associated with the Internet are usually not specifically caused by the Internet itself. The result can be uninvited browsing, copying or the destruction of valuable information, not to mention the rapid widespread migration of viruses. The most prevalent vulnerability is the reliance on user passwords. They provide a weak security mechanism that can be exploited. Another is the lack of security knowledge and training of users and system managers. The relatively simple exploitation by hackers of vulnerabilities in operating systems or application code is also a concern.

Portable PCs / Laptops

These days, many government officials, senior corporate executives and sales negotiators travel abroad with their own communication terminals such as a laptop with its own fax/data modem. It is no longer necessary to travel with bulky and heavy quantities of documents which can be instantly recalled from the home office. During business negotiations, a vast amount of technical details concerning, for instance, bidding information, client lists and negotiation strategies, can now be made available over a telephone line. These lines can be subjected to attack or interception by a competitor or foreign state.

Laptop computers are increasingly prime targets for theft, especially for domestic and international travellers. Travellers who anticipate carrying such items should be particularly wary while transiting airports and be alert to any sudden diversions. Two recent incidents at separate airports show the modus operandi of thieves operating in pairs that target laptop computers:

- While waiting to go through the security check at the x-ray machines, a traveller was preceded by the first thief, who then loitered around the area where security examines carry-on luggage. When the traveller placed his laptop computer on the conveyor belt of the x-ray machine, the second thief stepped in front of the traveller and set off the metal detector. With the traveller now delayed, the first thief removed the traveller's laptop from the conveyor belt just after it passed through the x-ray machine, and disappeared;

- A traveller carrying a laptop computer in his roll bag did not notice a thief position himself to walk in front of him. The thief stopped abruptly as the traveller passed by a crowd of people, causing the traveller also to stop. A second thief, who was following close behind, quickly removed the traveller's laptop and disappeared into the crowd.

Information Operations

One of the main problems with Information Operations (IO) is that there exists a wide variety of definitions. Initially the term Information Warfare (IW), coined by the American military, was used. Overtime, IW was replaced with IO, a term which included scenarios which could be applied outside the military theatre.

Generally speaking, IO can be defined as any tool or technique used to identify and/or exploit the vulnerabilities of any computer infrastructure, including government departments, commercial

entities, institutions, groups, and individuals for a variety of reasons, dependant on the intent of the user.

IO tools and techniques could be used by foreign governments, terrorist and extremist groups, or lone, politically - motivated individuals to do anything from steal proprietary information and technology, to launching an attack against Canada's critical infrastructures such as banking systems, airport air traffic systems, and power grids.

IO opens new horizons of cost effectiveness for terrorists and hostile foreign governments. IO is not only a relatively cheap and feasible means of attack, but it can originate thousands of miles away from an intended target. An offender can attack information with, in comparison to the damage, a modest investment of finance and equipment.

Today's society is increasingly dependent on interconnected infrastructures which, if destroyed, could adversely affect Canada's national security and economic stability.

Type of Threats

For most organizations, the major threat to computers remains internal. This includes disgruntled or dishonest employees who have the knowledge and the access needed to subvert corporate information systems. According to a 1998 Computer Security Institute (CSI) survey on information security, 44% of respondents reported hacking attempts from inside their organization making this the biggest threat to information security leading to security breaches.

Of increasing concern are casual hackers with social or political motives. An American juvenile computer hacker pleaded guilty to disabling a Worcester airport control tower and other airport facilities for six hours and disrupting phone service in Rutland, Massachusetts on 1997 03 10. The unidentified juvenile also hacked into a Worcester pharmacy computer and stole prescription details from a local chemist. Both attacks occurred when computer systems were made accessible through the Internet so that system administrators could work remotely.

Also, organized crime is using computers and there are some indications that the computer criminals are hooking up with hackers for illegal activities based on greed. In September 1996, Russian hackers apparently succeeded in siphoning about $10 million (U.S.) into foreign bank accounts, but bungled their attempts to extract cash from these electronic, fraudulent deposits. All but $400,000 (U.S.) of the stolen funds were recovered.

Security

Internet security can parallel the security concept we use every day. We lock our doors and windows in our houses for safety. Internet security (or any other information networks and standalone PCs) should follow the same philosophy. An organization must secure all access points between an internal network and the outside world and cannot rely on any security mechanism which it does not control. Completely securing the Internet is an impossible task and an easy step-by-step checklist for Internet security cannot exist when attacks are constantly changing. There are methods, techniques and guidelines that can reduce the risk considerably, and those who remember that keeping systems "secure" is an ongoing program can counter most problems.

Hackers will find and attack the weakest and most easily exploitable point of a network. Usually this is the initial point of contact within the company, its computer network. One way to prevent some of the corporate information from "leaking out" is to ensure that Internet terminals are completely separated from the company's other computer systems. Without a direct link to the company's operating systems, a potential hacker will only get into the company's Internet computer and not its core computer system. When risk is assessed as too high, the only safe connection to the Internet is none at all.

Every organization that connects computers to the Internet (or any other external networks) should develop a security policy for each of its systems. The policy should consist of directives or rules which reflect the organization's overall view on what is allowed and what is not. It should describe the types of access available, the applications allowed to be run, and who is allowed

access. The directives should be an analysis of the assets of an organization's system, and should assess the impact of a loss or compromise of a system, as well as the threats the system needs to be protected from. Identification authentication, accountability (audit), confidentiality, integrity and availability concerns should all be considered when setting a security policy. This policy should be unique for each system, and should be reviewed when changes in the system or organization occur.

Conclusion

On a global scale, a country's critical infrastructures are vulnerable to a malevolent individual, group or foreign government intent on destruction. On a smaller scale, private citizens and corporation are also susceptible to an IO attack. With a greater awareness of Internet and communications security by individuals, the last vestiges of such security through obscurity are fast disappearing.

Communications interception is no longer just the collection of information. Smaller countries around the world through the use of the Internet can now set up collation and analysis capabilities that a number of years ago were non-existent.

The interest of many governments in unscrupulously collecting and using commercial information either to assist negotiations in which they are engaged, or to enhance the competitiveness of their industries, has increased measurably over the last few years.

There is ample evidence that burglary and electronic surveillance have sometimes been used to serve a competitive business interest. However, for some governments and for most of the world's business community, there is only a recent realization that, without reasonably advanced security precautions, their sensitive information is vulnerable to unscrupulous agencies.

April 1998

Comments on this brief are welcome, and should be directed to the National Coordinator, Economic and Information Security, Box 9732, Station "T", Ottawa, K1G 4G4, phone (613) 231-0100, fax (613) 842-1390. If you'd like to talk to CSIS regarding a particular security concern, please contact the local Economic and Information Security Coordinator at one of the CSIS offices listed below:

Newfoundland ..... (709) 772-5449

Nova Scotia ..... (902) 420-5900

New Brunswick ..... (506) 452-3786

Quebec
- Montreal ..... (514) 393-5600
- Quebec City ..... (418) 529-8926

Ontario
- Ottawa ..... (613) 998-1679
- Toronto ..... (416) 865-1480

Manitoba ..... (204) 983-5405

Saskatchewan ..... (306) 780-5512

Alberta
- Edmonton ..... (403) 421-5800
- Calgary ..... (403) 292-5255

British Columbia ..... (604) 528-7400

BULLETIN DE SENSIBILISATION

Sécurité informatique

Le défi de la sécurité des systèmes d'information

Note de la rédaction :

Le précédent bulletin, intitulé *Espionnage économique : Faire des affaires sur le marché international* (avril 1998), décrit quelques-unes des méthodes préjudiciables aux intérêts du Canada qui sont employées dans le domaine de l'espionnage économique. Celui-ci met l'accent sur quelques-uns des aspects de la sécurité informatique touchant les personnes et les organisations qui misent de plus en plus sur la technologie de l'information pour la conduite de leurs affaires. Les organisations canadiennes peuvent se prémunir contre l'espionnage économique si elles connaissent bien les problèmes liés à la sécurité informatique et si elles prennent à cet égard des mesures adéquates pour se protéger.

Le présent bulletin est publié dans le cadre du Programme national de liaison et de sensibilisation du SCRS, dont l'objectif est d'établir avec les secteurs public et privé un dialogue permanent sur les menaces aux intérêts du Canada décrites ci-après l'espionnage économique animé par les gouvernements étrangers.

Introduction

Les progrès des télécommunications et de l'ordinatique ont suscité une révolution qui, en matière d'information, pourrait avoir une portée aussi grande que la révolution industrielle du XIX^{e} siècle. L'évolution rapide des réseaux téléphoniques et de ceux du câble, des satellites et des ordinateurs, ainsi que des logiciels, combinée aux percées technologiques dans le domaine du traitement informatique, a rendu possible cette dernière révolution.

Mis à part les changements rapides des ordinateurs personnels (OP), l'environnement informatique actuel permet une liaison poussée et complexe des OP, des réseaux et des serveurs. Nombre d'organisations ont maintenant des OP rattachés à différents réseaux et ont aussi accès à un gros ordinateur. L'ordinateur portatif et le bloc-notes augmentent les risques, car ils permettent de subtiliser facilement aux employeurs des informations confidentielles. La perte de ces informations, qu'elle soit délibérée ou accidentelle, peut coûter beaucoup plus cher qu'un gros ordinateur.

L'Internet

L'Internet est un réseau mondial qui relie des milliers de réseaux différents d'ordinateurs et des millions d'ordinateurs à l'échelle planétaire. De l'outil relativement obscur qu'il était pour les scientifiques et les chercheurs, il a acquis en 20 ans ses lettres de noblesse comme moyen

populaire, rentable et facile à utiliser pour communiquer et échanger de l'information. Des millions de gens emploient l'Internet pour brasser des affaires et des millions d'autres, pour se distraire.

Depuis plusieurs années, le nombre d'internautes fait plus que doubler chaque année, atteignant aujourd'hui quelque 40 millions répartis dans presque tous les pays du monde. Les connexions se multiplient de plus en plus rapidement, un nouveau réseau se greffant à l'Internet toutes les 30 minutes environ.

L'Internet se voulant un écheveau sans fin de réseaux, il est devenu presque impossible de discerner la fin d'un réseau et le début de l'autre. Ainsi, les réseaux des administrations municipales, provinciales et fédérale sont rattachés aux réseaux commerciaux qui, à leur tour, sont reliés aux réseaux militaires, financiers, à ceux des services publics, etc.
Le seul matériel requis pour accéder à l'Internet est un OP doté d'un modem et relié à une ligne téléphonique. Étant donné que de plus en plus de gens possèdent ce matériel, le mode de communication commode, économique, rapide et fascinant qu'est l'Internet devient de jour en jour plus attrayant. Comme le nombre d'internautes augmente, la masse de l'information offerte (dans les cybergroupes, émissions, fichiers de données, documents graphiques et multimédias et documents des gouvernements et de l'industrie, p. ex.) ne cesse de grandir et attire toujours plus d'utilisateurs.

Les problèmes de sécurité liés à l'Internet ne dépendent habituellement pas d'Internet même. Il est possible que des individus parcourent, copient ou détruisent sans autorisation de précieuses informations, sans compter la propagation rapide de virus. Le danger le plus courant vient des mots de passe qui sont un piètre mécanisme de sécurité, facilement exploitable. Un autre danger est le manque de connaissances et de formation des utilisateurs et des gestionnaires de systèmes sur le plan de la sécurité. D'autres préoccupations tiennent au fait que les pirates informatiques peuvent assez facilement tirer parti des points faibles des systèmes d'exploitation ou des codes d'application.

Les OP portatifs

De nos jours, beaucoup de fonctionnaires, de cadres supérieurs d'entreprise et de négociateurs de marchés voyagent en emportant avec eux leur propre terminal de télécommunication, comme un OP portatif doté d'un modem télécopieur. Cela leur évite de s'encombrer de lourds porte-documents puisqu'ils peuvent rappeler instantanément ces documents de leur bureau à domicile. Dans les négociations d'affaires, il est maintenant possible d'obtenir par liaison téléphonique une grande quantité de détails techniques : renseignements sur les soumissions, listes de clients et stratégies de négociation. Des sociétés concurrentes ou des États étrangers peuvent toutefois pirater ces liaisons.

Les ordinateurs portatifs sont de plus en plus convoités par les voleurs, surtout ceux que leurs propriétaires emportent sur des vols intérieurs ou internationaux. Ceux qui se munissent ainsi de leur OP doivent être particulièrement prudents dans les aéroports et demeurer aux aguets de toute diversion soudaine. Deux incidents survenus récemment dans des aéroports différents montrent que les voleurs qui s'en prennent aux ordinateurs portatifs travaillent en tandem :

- Attendant en file la vérification de sécurité devant les appareils de radioscopie, un voyageur avait été devancé par un premier voleur qui s'attardait alors près de l'endroit où le personnel de la sécurité examine les bagages à main. Dès que le voyageur eut placé son ordinateur portatif sur le tapis transporteur de l'appareil de radioscopie, le second voleur est passé devant lui et a déclenché le détecteur de métal, ce qui a empêché le voyageur de passer. Le premier voleur s'est alors emparé de l'ordinateur portatif, à sa sortie de l'appareil de radioscopie, puis il a disparu;

- Un voyageur transportant un ordinateur portatif dans un sac polochon n'avait pas remarqué qu'un voleur s'apprêtait à passer devant lui. Celui-ci s'est arrêté brusquement au moment où le voyageur passait près d'une foule, l'obligeant à s'immobiliser lui aussi. Un deuxième voleur, qui talonnait le voyageur, s'est alors vivement emparé de l'ordinateur portatif de ce dernier et s'est évanoui dans la foule.

Les opérations informatiques

L'une des principales difficultés que posent les opérations informatiques est qu'il existe une grande variété de définitions pour cette expression. On parlait initialement de la guerre de l'information, expression inventée par l'armée américaine. Au fil du temps, « guerre de l'information » a été remplacée par « opérations informatiques », expression qui s'applique à des scénarios en dehors du contexte militaire.

De façon générale, les opérations informatiques peuvent être définies comme étant tout instrument ou technique utilisé pour déceler et exploiter les faiblesses d'une infrastructure informatique, que ce soit celle d'un ministère, d'une entité commerciale, d'un établissement, d'un groupe ou d'un individu, à diverses fins selon l'intention de l'utilisateur.

Des instruments et techniques d'opérations informatiques pourraient être utilisés par des gouvernements étrangers, des groupes terroristes et extrémistes, ou des individus agissant seul et dont les motifs ont un caractère politique, pour commettre divers actes comme voler des informations et des technologies exclusives ou lancer une attaque contre les infrastructures essentielles du Canada, telles que les systèmes bancaires, les systèmes de contrôle de la circulation aérienne et les réseaux électriques.

Les opérations informatiques offrent de nouvelles perspectives de rentabilité pour les terroristes et les gouvernements étrangers hostiles. En plus de constituer un moyen d'attaque relativement économique et d'être assez faisables, elles peuvent être menées à des milliers de kilomètres de la cible visée. La mise de fonds et l'équipement nécessaires pour perpétrer un attentat contre des informations sont négligeables comparativement aux dommages qui peuvent en résulter.

La société d'aujourd'hui dépend de plus en plus d'infrastructures reliées entre elles, dont la destruction pourrait compromettre la sécurité nationale et la stabilité économique du Canada.

Type de menaces

Pour la plupart des organisations, la principale menace informatique demeure de source interne. Elle provient d'employés mécontents ou malhonnêtes qui ont les connaissances et l'accès nécessaires pour bouleverser les systèmes d'information de leur employeur. D'après un sondage de 1998 du Computer Security Institute (CSI) concernant la sécurité informatique, 44 % des personnes interrogées ont signalé des tentatives de piratage faites au sein même de leur organisation; ces tentatives constituent ainsi la plus grosse menace pour la sécurité de l'information menant à des infractions à la sécurité.

Les pirates informatiques occasionnels aux visées sociales ou politiques suscitent de plus en plus de craintes. Un pirate informatique américain encore mineur a plaidé coupable lorsqu'il a été accusé d'avoir mis hors d'état pendant six heures la tour de contrôle à l'aéroport de Worcester et d'autres installations de l'aéroport et d'avoir perturbé le service téléphonique à Rutland (Massachusetts) le 1997 03 10. Le jeune non identifié a aussi pénétré l'ordinateur d'une pharmacie de Worcester et volé des détails d'ordonnances à un chimiste de l'endroit. Les deux attaques ont eu lieu à partir du moment où des mesures ont été prises pour permettre l'accès par l'Internet aux systèmes informatiques de manière que les administrateurs des systèmes puissent travailler à distance.

Le grand banditisme se sert aussi d'ordinateurs, et certains indices donnent à penser que la cupidité amène les escrocs informatiques à s'aboucher avec les pirates informatiques pour mener des activités illégales. En septembre 1996, des pirates informatiques russes ont apparemment réussi à faire passer environ 10 millions de dollars US dans des banques étrangères, mais ils n'ont pu mettre la main sur ces dépôts électroniques frauduleux. Tous les fonds volés, moins 400 000 $US, ont été recouvrés.

Sécurité

La sécurité sur l'Internet peut s'inspirer des principes courants, comme celui qui nous incite à verrouiller portes et fenêtres de nos maisons. Qu'il s'agisse de l'Internet (ou de tout autre réseau d'information et d'un OP autonome), la sécurité doit respecter les mêmes principes. Toute organisation doit protéger l'ensemble des points d'accès entre son réseau interne et le monde extérieur et ne peut compter sur les mécanismes de sécurité qui ne sont pas de son ressort. Une sécurité étanche de l'Internet est impossible et nulle procédure facile ne saurait permettre de l'assurer étant donné que les menaces prennent sans cesse de nouvelles formes. Certaines méthodes, techniques et lignes directrices peuvent réduire les risques considérablement et ceux qui en sont conscients et « protègent » leurs systèmes en tout temps peuvent éviter la plupart des problèmes.

Les pirates informatiques savent trouver le chaînon le plus faible et le plus facilement exploitable d'un réseau et en tirer parti. Il s'agit généralement du premier point de contact avec une entreprise : son réseau informatique. Pour une entreprise, une façon d'éviter la « fuite » d'une partie de son information est de veiller à ce que ses terminaux reliés à l'Internet soient complètement à part de tous ses autres systèmes informatiques. Sans un lien direct avec ces systèmes d'exploitation, un pirate informatique ne peut accéder qu'à l'ordinateur branché sur l'Internet, mais non pas au système informatique central. Si la société juge les risques trop élevés, la seule façon d'assurer la sûreté des connexions à l'Internet est de n'en établir aucune.

Toute organisation qui a des ordinateurs reliés à l'Internet (ou à tout autre réseau externe) doit élaborer une politique pour assurer la sécurité de chaque système. Cette politique doit énoncer des directives ou règles qui traduisent la conception globale de l'organisation quant à ce qui est permis et à ce qui ne l'est pas. Elle doit décrire les types d'accès offerts, les applications permises et les personnes jouissant d'une autorisation d'accès. Ces directives doivent faire l'analyse des biens contenus dans le système de l'organisation et évaluer les conséquences de la perte d'un système ou de l'intrusion dans celui-ci ainsi que les menaces dont il faut protéger chaque système. Toute politique relative à la sécurité doit tenir compte des divers aspects suivants : authentification de l'identité, responsabilité (vérification), confidentialité, intégrité et disponibilité. Elle doit être propre à chaque système et être revue à chaque modification d'un système ou de l'organisation même.

Conclusion

À l'échelle mondiale, les infrastructures essentielles d'un pays risquent d'être prises pour cibles par un individu, un groupe ou un gouvernement étranger malveillant qui voudrait les détruire. Sur une plus petite échelle, les particuliers et les entreprises sont susceptibles eux aussi d'être victimes d'une opération informatique. Comme tout le monde est plus conscient de la sécurité de l'Internet et des communications, les derniers vestiges d'une telle sécurité fondée sur l'obscurité sont en voie de disparaître rapidement.

L'interception des communications ne se limite plus à la collecte d'information. Grâce à l'Internet, de petits pays ont maintenant une capacité de collecte et d'analyse qui n'existait pas il y a quelques années.

Ces dernières années, on a noté une augmentation sensible du nombre de gouvernements qui cherchent davantage à recueillir et à utiliser sans scrupules des renseignements commerciaux, soit pour faciliter leurs propres négociations, soit pour transmettre cette information à leurs entreprises nationales engagées dans une lutte concurrentielle.

Il existe de nombreuses preuves de recours occasionnels au cambriolage et à la surveillance électronique, visant à soutenir une telle lutte. Cependant, certains gouvernements et la majorité des milieux d'affaires du monde viennent à peine de se rendre compte que, sans mesures de sécurité assez poussées, leur information délicate est à la merci d'organisations et de gouvernements sans vergogne.

avril 1998

N'hésitez pas à nous faire part de vos commentaires sur ce bulletin. Veuillez les adresser au coordonnateur national des questions de sécurité économique et de l'information, C.P. 9732, Succursale postale «T», Ottawa, K1G 4G4, téléphone (613) 231-0100, télécopieur (613) 842-1390. Si vous souhaitez discuter d'une question particulière, veuillez communiquer avec le coordonnateur des questions de sécurité économique et de l'information de l'un des bureaux régionaux suivants du SCRS :

Terre-Neuve ..... (709) 772-5449

Nouvelle-Écosse ..... (902) 420-5900

Nouveau-Brunswick ..... (506) 452-3786

Québec
- Montréal ..... (514) 393-5600
- Québec ..... (418) 529-8926

Ontario
- Ottawa ..... (613) 998-1679
- Toronto ..... (416) 865-1480

Manitoba ..... (204) 983-5405

Saskatchewan ..... (306) 780-5512

Alberta
- Edmonton ..... (403) 421-5800
- Calgary ..... (403) 292-5255

Colombie-Britannique ..... (604) 528-7400